

ROUTING AND TRANSMITTAL SLIP

22 JAN 86

TO: (Name, office symbol, room number, building, Agency/Post)

1. DIRECTOR OF INFORMATION SERVICES

2.

3.

4.

5.

Action	File	Note and Return
Approve	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

#1 - ACTION

FOR APPROPRIATE ACTION/RESPONSE. THE REPORTED
NONCOMPLIANCE WITH NSDD 84 IS AN ISSUE OF CONTENTION
AND THE SUBJECT OF CORRESPONDENCE TO NSC.

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, office symbol, Agency/Post)

Room No.—Bldg.

Phone No.

1041-102

*USGPO 1963-421-529/320

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

EXECUTIVE SECRETARIAT
ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI		X		
2	DDCI		X		
3	EXDIR		X		
4	D/ICS				
5	DDI				
6	DDA	X			
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC		X		
11	IG				
12	Compt				
13	D/OLL				
14	D/PAO				
15	D/PERS				
16	VC/NIC				
17	D/OIS/DDA		X		
18	D/Security		X		
19					
20					
21					
22					

SUSPENSE _____ Date _____

Remarks

To 6: Yours for appropriate action/response.
The reported noncompliance with NSDD 84 is an issue
of contention and the subject of correspondence
to NSC.

Executive Secretary

16 Jan 86

Date

3637 (10-81)



General
Services
Administration
Information Security
Oversight
Office

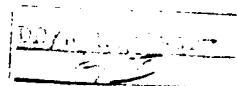
Washington, DC 20405

Executive Registry

66-0222x

January 9, 1986

Honorable William J. Casey
Director of Central Intelligence
Central Intelligence Agency
Washington, DC 20505



Dear Mr. Casey:

Sections 5.2(b)(2) and (4) of Executive Order 12356 authorize the Information Security Oversight Office (ISOO) to conduct on-site reviews of the information security programs of executive branch agencies that generate or handle national security information. To comply with the Order's requirements, Harold Mason, ISOO Program Analyst, conducted a review of the information security program in a number of offices in the Central Intelligence Agency (CIA) during FY 1985. A list of offices visited is contained in the appendix to the enclosed report. This report complements the report of April 29, 1985.

Mr. Mason examined several aspects of the program at CIA, including classification, security education, and safeguarding. The results of the ISOO review are contained in the enclosed report. Mr. Mason found the CIA offices visited to be in compliance with the Order; however, the CIA has failed to implement the provisions of National Security Decision Directive 84 by failing either to implement the Standard Form 189, Classified Information Nondisclosure Agreement, or to seek a waiver of its use through the ISOO from the National Security Council.

waiver being sought

I appreciate the excellent cooperation of [redacted] and other officials with whom Mr. Mason met. If you have any questions on the enclosed report, please contact me on 535-7251.

Sincerely,

STEVEN GARFINKEL
Director

Enclosure

Report of Inspection by the
Information Security Oversight Office of the
Central Intelligence Agency

I. General

During Fiscal Year 1985, Harold Mason, Program Analyst, Information Security Oversight Office (ISOO), inspected five offices in the Central Intelligence Agency (CIA), to evaluate their information security program and their compliance with Executive Order 12356 and ISOO implementing Directive No. 1. [redacted] Agency Security Classification Officer, assisted Mr. Mason during the course of the inspection and coordinated with the offices inspected. A list of offices inspected is included in the appendix. This report complements the report of April 29, 1985.

II. Findings

A. Classification

The Agency continues to use its classification guide as a basis for derivative classification. The offices inspected have had sufficient experience in using the combined classification guide that replaced the individual guides used for each directorate. None of the personnel visited expressed any concern or encountered any significant problem in its use. The only problem encountered in derivative classification, in FY 1985, was reported in the ISOO inspection report of April 29, 1985, to the Director. The ISOO was informed that the problem would be resolved by utilizing the ISOO-produced slide presentation on classification marking.

B. Training

Personnel continue to receive extensive initial and refresher training by the Office of Training and Education on security, safeguarding, marking, and a wide variety of subjects. In addition, many of the offices provide additional training oriented to the directorate and office of assignment. Personnel are routinely monitored for the proper handling and safeguarding of classified information.

C. Safeguarding

The CIA has an excellent program for the handling, storage, and transmittal of classified information. The Agency routinely reviews and updates its

Enclosure

distribution list to determine if the recipients continue to have a need-to-know. No deficiency in safeguarding procedures was detected during the course of the inspection.

D. Standard Form 189

Paragraph 1.a. of National Security Decision Directive 84 (NSDD-84), "Safeguarding National Security Information," signed by the President on March 11, 1983, states: "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive." Paragraph 1.c. of the Directive further states: "All agreements required in paragraphs 1.a. . . . must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (ISOO), shall develop standardized forms that satisfy these requirements."

In order to fulfill his responsibility under the Directive and Section 5.2(b)(7) of Executive Order 12356, the Director of ISOO published regulations regarding the Classified Information Nondisclosure Agreement, SF 189, in the Federal Register, vol. 48, no. 176, September 9, 1983, 32 CFR Part 2003. The use of the standard form is mandatory for all departments and agencies or offices of the executive branch that create and/or handle national security information. The Register states: "Only the National Security Council may grant an agency's application for a waiver from the use of SF 189. To apply for a waiver, an agency must submit its proposed alternative nondisclosure agreement to the Director of ISOO, along with its justification. The Director of ISOO will request a determination about the alternative agreement's enforceability from the Department of Justice prior to making a recommendation to the National Security Council."

The CIA has failed to require its employees to sign the SF 189 or request a waiver. If the CIA believes that its present nondisclosure form meets or exceeds SF 189 and desires to continue to use its own form, then a waiver must be requested. If no waiver is requested, then the CIA should immediately implement the provisions of NSDD-84 and require its employees to sign SF 189.

3

In its upcoming report to the President for FY 1985, ISOO has been asked to include an update on agency-by-agency implementation of the SF 189. The CIA will be noted as having taken no action on it.

III. Conclusion

The CIA's information security program is in compliance with Executive Order 12356 and the ISOO Directive No. 1, but the Agency has failed to implement the provisions of NSDD-84 by failing either to implement the SF 189 or to seek a waiver of its use.

IV. Recommendation

Expedite the signing of SF 189 by CIA employees, or request a waiver from its use.

FYI

ADDA

DDA

(DDA Registry for File)

Appendix

**CIA Offices
Inspected in Fiscal Year 1985**

**Office of Scientific and Weapons Research, Deputy Director for
Intelligence**

Office of the Comptroller

Office of Communications

Security Education Group

Directorate of Operations branch components and offices

3a

REFERENCE

EXECUTIVE SECRETARIAT

Routing Slip

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI		<input checked="" type="checkbox"/>		
2	DDCI		<input checked="" type="checkbox"/>		
3	EXDIR		<input checked="" type="checkbox"/>		
4	D/ICS		<input checked="" type="checkbox"/>		
5	DDI		<input checked="" type="checkbox"/>	14 Jun 83	
6	DDA	<input checked="" type="checkbox"/>			
7	DDO		<input checked="" type="checkbox"/>		
8	DDS&T		<input checked="" type="checkbox"/>		
9	Chm/NIC		<input checked="" type="checkbox"/>		
10	GC	<input checked="" type="checkbox"/>			
11	IG		<input checked="" type="checkbox"/>		
12	Compt		<input checked="" type="checkbox"/>		
13	D/EEO		<input checked="" type="checkbox"/>		
14	D/Pers		<input checked="" type="checkbox"/>		
15	D/OEA		<input checked="" type="checkbox"/>		
16	C/PAD/OEA				
17	SA/IA				
18	AQ/DCI		<input checked="" type="checkbox"/>		
19	C/IPD/OIS				
20	C/STORM	<input checked="" type="checkbox"/>			
21	CCC		<input checked="" type="checkbox"/>		
22	C/CCS/BCS		<input checked="" type="checkbox"/>		
SUSPENSE				Date	

Remarks: NIO/FDIA

X (31 Oct 85)

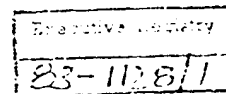
Executive Secretary
15 March 19

Date

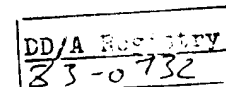
3-37 (10-81)

THE WHITE HOUSE

WASHINGTON



March 11, 1983



MEMORANDUM FOR THE VICE PRESIDENT
 THE SECRETARY OF STATE
 THE SECRETARY OF THE TREASURY
 THE SECRETARY OF DEFENSE
 THE ATTORNEY GENERAL
 THE SECRETARY OF INTERIOR
 THE SECRETARY OF AGRICULTURE
 THE SECRETARY OF COMMERCE
 THE SECRETARY OF LABOR
 THE SECRETARY OF HEALTH AND HUMAN SERVICES
 THE SECRETARY OF HOUSING AND URBAN DEVELOPMENT
 THE SECRETARY OF TRANSPORTATION
 THE SECRETARY OF ENERGY
 COUNSELLOR TO THE PRESIDENT
 THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
 THE DIRECTOR OF CENTRAL INTELLIGENCE
 UNITED STATES REPRESENTATIVE TO THE UNITED NATIONS
 UNITED STATES TRADE REPRESENTATIVE
 CHIEF OF STAFF TO THE PRESIDENT
 DEPUTY CHIEF OF STAFF TO THE PRESIDENT
 ASSISTANT TO THE PRESIDENT FOR POLICY DEVELOPMENT
 DIRECTOR, WHITE HOUSE MILITARY OFFICE
 CHAIRMAN, PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY
 BOARD
 CHAIRMAN, PRESIDENT'S INTELLIGENCE OVERSIGHT BOARD
 CHAIRMAN, COUNCIL OF ECONOMIC ADVISERS
 CHAIRMAN, COUNCIL ON ENVIRONMENTAL QUALITY
 CHAIRMAN, JOINT CHIEFS OF STAFF
 CHAIRMAN, NUCLEAR REGULATORY COMMISSION
 ADMINISTRATOR, AGENCY FOR INTERNATIONAL DEVELOPMENT
 DIRECTOR, ARMS CONTROL AND DISARMAMENT AGENCY
 DIRECTOR, OFFICE OF SCIENCE AND TECHNOLOGY
 ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION
 DIRECTOR, UNITED STATES INFORMATION AGENCY
 ADMINISTRATOR, NATIONAL AERONAUTICS AND SPACE
 ADMINISTRATION
 ADMINISTRATOR, ENVIRONMENTAL PROTECTION AGENCY
 DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
 DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY

L 117

NSDD 84

XF NSDD 119

 DCI
 EXEC
 REG

DIRECTOR, NATIONAL SCIENCE FOUNDATION
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, OFFICE OF PERSONNEL MANAGEMENT
DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE

SUBJECT: NSDD-84: Safeguarding National Security Information

The President has approved the attached National Security Decision Directive on safeguarding national security information. The Director of the Information Security Oversight Office shall distribute copies of the Directive to any agency not listed above that originates or handles national security information.

FOR THE PRESIDENT:



William P. Clark

Attachment

NSDD-84

THE WHITE HOUSE

WASHINGTON

March 11, 1983

National Security Decision
Directive Number 84

Safeguarding National Security Information

As stated in Executive Order 12356, only that information whose disclosure would harm the national security interests of the United States may be classified. Every effort should be made to declassify information that no longer requires protection in the interest of national security.

At the same time, however, safeguarding against unlawful disclosures of properly classified information is a matter of grave concern and high priority for this Administration. In addition to the requirements set forth in Executive Order 12356, and based on the recommendations contained in the interdepartmental report forwarded by the Attorney General, I direct the following:

1. Each agency of the Executive Branch that originates or handles classified information shall adopt internal procedures to safeguard against unlawful disclosures of classified information. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information. All such agreements must include a provision for prepublication review to assure deletion of SCI and other classified information.

c. All agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (ISOO), shall develop standardized forms that satisfy these requirements.

d. Appropriate policies shall be adopted to govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures of classified information. All persons with authorized access to classified information shall be clearly apprised of the agency's policies in this regard.

2. Each agency of the Executive branch that originates or handles classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

e. Persons determined by the agency to have knowingly made such disclosures or to have refused cooperation with investigations of such unauthorized disclosures will be denied further access to classified information and subjected to other administrative sanctions as appropriate.

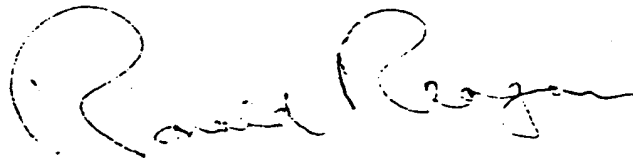
3. Unauthorized disclosures of classified information shall be reported to the Department of Justice and the Information Security Oversight Office, as required by statute and Executive orders. The Department of Justice shall continue to review reported unauthorized disclosures of classified information to determine whether FBI investigation is warranted. Interested departments and agencies shall be consulted in developing criteria for evaluating such matters and in determining which cases should receive investigative priority. The FBI is authorized to investigate such matters as constitute potential violations of federal criminal law; even though administrative sanctions may be sought instead of criminal prosecution.

4. Nothing in this directive is intended to modify or preclude interagency agreements between FBI and other criminal investigative agencies regarding their responsibility for conducting investigations within their own agencies or departments.

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate

adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations, and guidelines.

A handwritten signature in dark ink, appearing to read "Ronald Reagan". The signature is written in a cursive, flowing style with a large initial "R".